TUESDAY, FEBRUARY 18, 2020 | SERVING CHICAGO'S LEGAL COMMUNITY FOR 164 YEARS | CHICAGOLAWBULLETIN.COM

Chicago Daily Law Bulletin®

VOLUME 166, NO. 33

LAW BULLETIN MEDIA

Facial recognition cameras bring some good, some bad to sports

SPORTS
MARKETING PLAYBOOK

DOUGLAS N. MASTERS and SETH A. ROSE

DOUGLAS N. MASTERS *is a partner at Loeb & Loeb LLP, where he litigates and counsels clients primarily in intellectual property, advertising and unfair competition. He is co-chair of the firm's intellectual property protection group. dmasters@loeb.com*
SETH A. ROSE *is a partner at the firm, where he counsels clients on programs and initiatives in advertising, marketing, promotions, media, sponsorships, entertainment, branded and integrated marketing, and social media. srose@loeb.com*

Facial recognition systems have been part of the sports world for some time. Many venues, stadiums and team locker rooms have installed the technology to increase security as well as provide faster, easier access.

In fact, facial recognition technology will be a key part of security at the Tokyo 2020 Summer Olympic and Paralympic Games, where Tokyo-based NEC Corp. will provide a facial recognition platform that will store in a database the facial image of the estimated 300,000 athletes and staff, to increase safety and streamline security operations, according to the Tokyo Olympic Organizing Committee.

Sports teams and leagues also are deploying facial recognition for their own purposes, from ensuring fan and player safety to encouraging fan engagement on social media and creating VIP experiences for season ticket holders.

At the same time, however, concern about individual privacy — and in particular, privacy around biometric data, including face, fingerprint and retina scans — is growing, especially in the United States, where the regulatory framework for the most part has lagged behind the evolution of facial recognition software and biometric technology.

Security issues are the most practical reason for facial recognition technology. Sports organizations around the world notably use the technology to streamline security efforts, flag individuals who have been banned from venues and even identify fans responsible for inappropriate behavior.

Italian soccer league Serie A is fighting racism by, among other initiatives, developing facial recognition software to catch fans aiming offensive language and chants at black players.

The league has experienced an ongoing problem with this behavior in recent years, but the perpetrators have gone largely unpunished because of the difficulty in identifying them, according to The Associated Press.

As of the end of last year, the league said it was waiting on authorization from Italy's privacy authorities to use the software in stadiums.

In Denmark, Superliga football club Brøndby began using facial recognition technology in mid-2019 to beef up stadium security by automating the identification of people who have been banned from the venue. Up to 100 people may be on the stadium's blacklist at a time and security personnel previously had to personally keep an eye out for those individuals.

Now, security cameras and facial recognition software provided by Panasonic at the venue outside Copenhagen can scan people entering the stadium gates, quickly identify banned individuals and alert security personnel, Panasonic explained in a statement. With an average attendance of 14,000 people per game, the system will also decrease congestion at the gates and improve fans' experience.

The system can even recognize faces that are partially concealed by hats, scarves or sunglasses, Panasonic noted.

The city of Moscow took surveillance using facial recognition a step further by piloting a wide-ranging security initiative ahead of the 2018 World Cup. The city installed closed-circuit cameras in and around train stations near the stadium where the game between Russia and Spain would be played, The Moscow Times reported.

This facial recognition technology was credited with helping nab a Russian fan at the game who was wanted for theft, after approximately 50,000 photos were uploaded to the surveillance system at the stadium.

In the Unites States, the U.S. Tennis Association has been capitalizing on facial recognition technology to ferret out people transmitting real-time data on matches to give bettors and brokers an edge in sports gambling, ESPN reported.

Since 2016, the tennis association has used cameras to scan U.S. Open crowds for so-called courtsiders who were potentially involved in gambling corruption. The association suspected these individuals — some of whom have been known to wear disguises to avoid being recognized — were communicating information about the match, such as who won a certain point, to their partners, faster than official data feeds, giving some data brokers and bettors a competitive edge.

The association was able to ferret out at least 19 courtsiders in 2016, and at least one in 2018.

The association has monetized its real-time data since 2012, licensing their live streaming and data for the U.S. Open for use in legal betting around the world and the legalization of sport betting in the United States in the last two years will only make this data that much more valuable — and worth protecting even more.

Teams, leagues and venues are finding other ways to capitalize on collecting fan images as well. Marketers are gathering image-based information about fans to improve their onsite experience, to encourage fan engagement on social media and to provide enhanced data analytics to sponsors.

Across the sports world, teams and stadiums are partnering with technology companies to install cameras in the venues that photograph individual fans throughout events. These cameras can take photos, for example, of every seat in the stadium to capture a real-time view of attendee demographics.

Photo-centric data can be used to give season ticket holders VIP treatment, acknowledge birthdays and special events and tailor music selections depending on the demographics of the crowd attending that game, CNBC reported.

Facial recognition technology can also drive fan engagement. One of the features offered by South African tech company Fancam lets fans access photos of themselves at the game and encourages them to post the images on social media and tag themselves. It was rumored that the U.S. Tennis Association used its facial recognition technology to find celebrities in the stands.

Identifying and tracking people by their unique biometric attributes, including faces, fingerprints and retinas raises, concerns about privacy issues — and spawns litigation.

Proposed class actions filed by employees allege their employers are improperly collecting and using their fingerprints, while consumers argue that facial recognition technology used by social media and photo-sharing platforms invades users' privacy.

Illinois is ahead of the curve in regulation of biometric information collection. The state enacted the Biometric Information Privacy Act in 2008, the first law of its kind in the country and the only state law that includes a private right of action.

Texas and Washington state passed similar legislation, but without a private right of action.

The most significant decision to date under BIPA is the Illinois Supreme Court ruling in early 2019, which concluded that a plaintiff does not need to claim actual harm to bring a suit under the law. In *Rosenbach v. Six Flags Entertainment Corp.,* a mother sued the far north suburban Gurnee theme park for violating the BIPA after her son was fingerprinted without his written consent to access a season pass she had purchased for him. The theme park also failed to disclose what it does with the biometric data it collects, in violation of the law.

The use of facial recognition technology at live sporting events has the potential to spark calls for regulation or legislation and perhaps could lead to similar litigation. That is, at least in part, why the tennis association posts signs at a number of sponsored events putting attendees on notice about the possibility that their image, voice or likeness could be recorded and used.

No federal regulation currently covers the collection of biometric information. The American Civil Liberties Union filed a lawsuit in a Massachusetts federal court in October 2019 against the U.S. Department of Justice, the Drug Enforcement Administration and the FBI, seeking information about federal law enforcement's use of face recognition surveillance technology.

At issue is software provided to government customers and how the agencies use the biometric information they collect.

The ACLU also conducted an illuminating experiment with photos of professional athletes from Massachusetts sports leagues. Using a facial recognition software program, the ACLU compared the official headshots of 188 athletes from teams including the New England Patriots, the Boston Bruins, the Red Sox and the Celtics with a database of 20,000 mugshots, the website Boston.com reported.

The result? The software falsely matched the photos of 27 athletes with mugshots in the database. One of the players, Patriots safety Duron Harmon, is now publicly supporting a proposed moratorium on the use of facial recognition technology by Massachusetts government agencies, Boston.com noted.

Facial recognition initiatives by sports organizations in the United States and abroad are just getting started and will likely increase as stadiums, teams and leagues find compelling — and potentially lucrative — uses for this technology for security and beyond.

The use of facial recognition technology in Tokyo this summer will shine an even brighter global spotlight on the technology, including any issues and glitches. How fans will react will certainly be part of the ongoing story.